UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS

OFFICE OF INSPECTOR GENERAL

AUD-IT-14-33 Office of Audits September 2014

Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program

~~**IMPORTANT NOTICE**: This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies of organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

United States Department of State
and the Broadcasting Board of Governors

Office of Inspector General

(U) PREFACE

(U) This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

(U) This report is the result of an assessment of the strengths and weaknesses of the office, post, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observation, and a review of applicable documents.

(U) The recommendations therein have been developed on the basis of the best knowledge available to OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

(U) I express my appreciation to all of those who contributed to the preparation of this report.

(U) Norman P. Brown
(U) Assistant Inspector General
for Audits

(U) Acronyms

(U) FISMA	Federal Information Security Management Act
(U) GSS	General Support System
(U) IBWC	International Boundary and Water Commission
(U) NIST	National Institute of Standards and Technology
(U) OIG	Office of Inspector General
(U) SBIWTP	South Bay International Wastewater Treatment Plant
(U) SCADA	Supervisory Control and Data Acquisition
(U) SP	Special Publication

(U) Table of Contents

(U) Section **(U) Page**

(U) Executive Summary

(U) In accordance with the Federal Information Security Management Act of 2002[1] (FISMA), the Department of State (Department), Office of Inspector General (OIG), conducted an audit of the U.S. Section, International Boundary and Water Commission (IBWC), information security program and practices. The purpose of the audit was to determine compliance with Federal laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). In addition, OIG reviewed IBWC's corrective actions to address weaknesses identified in OIG's FY 2013 report.[2] OIG closed 22 of 27 recommendations in the FY 2013 report. The status of each recommendation from OIG's FY 2013 report is presented in Appendix B.

(U) During FY 2014, OIG conducted field work at IBWC's U.S. Section headquarters in El Paso, TX; South Bay International Wastewater Treatment Plant (SBIWTP) and field office in San Diego, CA; Nogales International Wastewater Treatment Plant in Nogales, AZ; Amistad Dam and field office in Del Rio, TX; and the General Support System (GSS) continuity of operations site in Las Cruces, NM.

~~(SBU)~~ Overall, OIG found that IBWC had implemented an information security program. The Information Management Division, led by its Information System Security Manager, with guidance from IBWC's Chief Administrative Officer and support from the Commissioner, made significant progress on previously identified weaknesses. For example, IBWC established a Continuous Security Monitoring program for its GSS, developed authorization packets for its GSS and Supervisory Control and Data Acquisition (SCADA) systems,[3] cleared multiple personnel requiring enhanced background investigations, developed contingency documentation, and implemented a multifactor authentication solution for logical access.

~~(SBU)~~ Notwithstanding the progress made by IBWC, OIG identified the following control weaknesses related to four security control areas:

- **~~(SBU)~~** [Redacted] (b) (5). (Finding A)
- **~~(SBU)~~** IBWC's [Redacted] (b) (5) policy. In addition, [Redacted] (b) (5) [Redacted] (b) (5). (Finding B)
- **~~(SBU)~~** IBWC had not [Redacted] (b) (5). (Finding C)

[1] **(U)** E-Government Act of 2002, Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (2002).

[2] **(U)** *Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program* (AUD/IT-13-39, September 2013).

[3] **(U)** A SCADA system performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data.

- ~~(SBU)~~ IBWC's [redacted]. In addition, IBWC included contractor-owned inventory in the Integrated Logistics Management System. (Finding D)

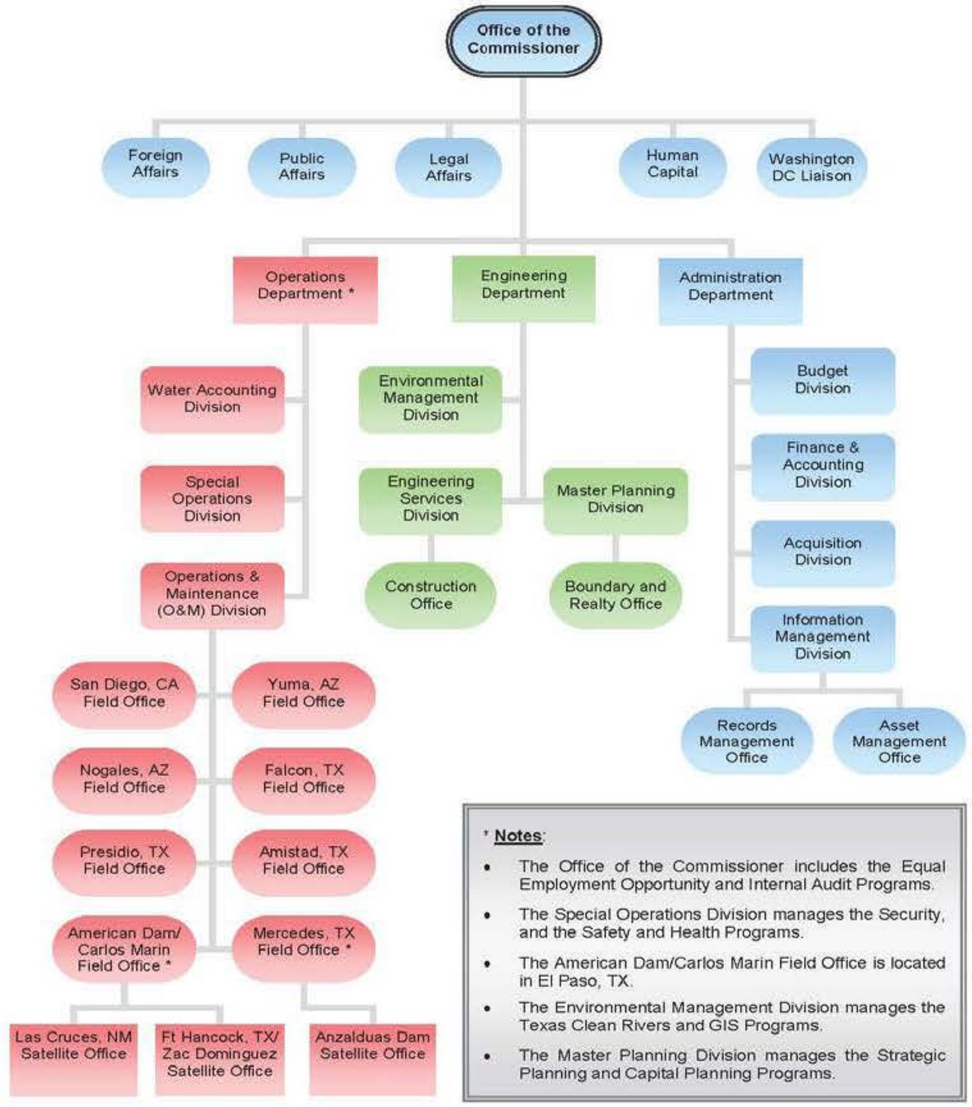
~~(SBU)~~ OIG made six recommendations to IBWC intended to improve its information security program and practices. In July 2014, OIG provided a draft of this report to IBWC. In its July 29, 2014, response (Appendix C) to the draft report, IBWC concurred with all six recommendations. Based on the comments received, OIG considers all six recommendations resolved, pending further action. IBWC's management responses to the recommendations and OIG's analysis to the responses are presented after each recommendation.

(U) Background

(U) IBWC is a binational commission, established to apply boundary and water treaties and agreements between the United States and Mexico. IBWC consists of a U.S. Section and a Mexican Section. The organization of IBWC's U.S. Section is shown in Figure 1. Each Section is administered independently of the other, and is headed by an Engineer Commissioner, who is appointed by his respective President. The U.S. Section receives foreign policy guidance from the U.S. Department of State, while the Mexican Section is administratively linked to the Secretariat of Foreign Relations of Mexico. The joint mission of the U.S. Section and the Mexican Section is as follows:

- **(U)** Distribute the waters of the boundary-rivers between the two countries.
- **(U)** Operate international flood control along the boundary-rivers.
- **(U)** Operate the international reservoirs for conservation and regulation of Rio Grande waters for the two countries.
- **(U)** Improve the quality of water of international rivers.
- **(U)** Resolve border sanitation issues.
- **(U)** Develop hydroelectric power.
- **(U)** Establish the boundary in the area bordering the Rio Grande.
- **(U)** Demarcate the land boundary.

(U) Figure 1. U.S. Section of IBWC Organizational Chart


Office of the Commissioner
Foreign Affairs
Public Affairs
Legal Affairs
Human Capital
Washington DC Liaison
Operations Department *
Engineering Department
Administration Department
Water Accounting Division
Special Operations Division
Operations & Maintenance (O&M) Division
Environmental Management Division
Engineering Services Division
Master Planning Division
Construction Office
Boundary and Realty Office
Budget Division
Finance & Accounting Division
Acquisition Division
Information Management Division
Records Management Office
Asset Management Office
San Diego, CA Field Office
Yuma, AZ Field Office
Nogales, AZ Field Office
Falcon, TX Field Office
Presidio, TX Field Office
Amistad, TX Field Office
American Dam/ Carlos Marin Field Office *
Mercedes, TX Field Office *
Las Cruces, NM Satellite Office
Ft Hancock, TX/ Zac Dominguez Satellite Office
Anzalduas Dam Satellite Office

* Notes:

- The Office of the Commissioner includes the Equal Employment Opportunity and Internal Audit Programs.
- The Special Operations Division manages the Security, and the Safety and Health Programs.
- The American Dam/Carlos Marin Field Office is located in El Paso, TX.
- The Environmental Management Division manages the Texas Clean Rivers and GIS Programs.
- The Master Planning Division manages the Strategic Planning and Capital Planning Programs.

(U) Source: This chart is an excerpt from the IBWC FY 2011-2016 Strategic Plan.

(U) The U.S. Section owns the contractor-operated SBIWTP, which is responsible for meeting the Clean Water Act requirements mandated by the State of California. The SBIWTP discharges the clean water into the Pacific Ocean. The U.S. Section also maintains and operates the Nogales International Wastewater Treatment Plant in accordance with the Clean Water Act discharge standards mandated by Arizona. Each wastewater treatment plant has a SCADA system. Based on information received from remote stations, automated or operator-driven supervisory commands are controlled by remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

(U) FISMA was enacted into law as Title III, Public Law Number 107-347, on December 17, 2002. Key requirements of FISMA are as follows:

- **(U)** The establishment of an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
- **(U)** An annual independent evaluation of the agency's information security programs and practices.
- **(U)** An assessment of compliance with FISMA requirements.

(U) FISMA assigns specific responsibilities to NIST, OMB, and the Department of Homeland Security and other Federal agencies for the purpose of strengthening information system security throughout the Federal Government. In particular, FISMA requires the head of each agency to implement policies and procedures to cost effectively reduce information technology security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to the Department of Homeland Security.

(U) The U.S. Section is developing and implementing information technology policies and procedures to meet requirements mandated by FISMA, OMB, and NIST for its information systems. The Section has also entered into agreements with third parties to help meet FISMA compliance.

(U) Objective

(U) The objective of the audit was to assess the effectiveness of IBWC's information security program in FY 2014. Specifically, OIG assessed risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, continuous monitoring, contingency planning, oversight of contractor systems, security capital planning, access controls, personnel security, and physical and environmental protection.

(U) Audit Results

(U) Finding A. [redacted]

~~(SBU)~~ For FY 2014, IBWC executed a contract with Aitheras, who subcontracted TruShield to perform [redacted] of its GSS. TruShield provided IBWC with weekly status updates and monthly vulnerability scans. However, IBWC had not [redacted] (b) (5)

~~(SBU)~~ [redacted] Although IBWC was aware of the NIST requirement for its SCADA systems, [redacted] Therefore, IBWC contracted Veolia to ensure the SCADA systems were FISMA compliant; however, Veolia did not perform the contractual work, which included [redacted]. Because Veolia had not performed the required work, IBWC utilized TruShield to develop [redacted] The SCADA [redacted] (b) (5) is currently in draft.

~~(SBU)~~ Without an [redacted] there is an increased risk that the [redacted] leading to potential damage or disruption to IBWC's SCADA systems. In addition, environmental hazards could occur resulting in fines and lawsuits for IBWC.[5]

> ~~(SBU)~~ **Recommendation 1.** OIG recommends that the International Boundary and Water Commission (IBWC [redacted], as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.
>
> ~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that it would obtain an [Redacted] (b) (5) [redacted]

[4] **(U)** NIST SP 800-53, rev. 3, "Recommended Security Controls for Federal Information Systems and Organizations," CA-7 [redacted] Aug. 2009 (last updated May 2010).

[5] **(U)** Lauren Steussy and Paul Krueger, "Sewage Flowed into Local Waters without Notice: Report," *NBC 7 San Diego*, April 12, 2012, <http://www.nbcsandiego.com/news/local/Sewage-Spilled-in-Local-Waters-without-Notice-147198795.html >, accessed on June 17, 2014.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts the [redacted] for each SCADA system.

(U) Finding B. [Redacted] (b) (5)

~~(SBU)~~ In FY 2014, IBWC established a testing process for changes to its GSS. However, IBWC determined that its [Redacted] (b) (5) because of the high availability and sensitivity requirements necessary for the system. Therefore, IBWC executed a contract[7] to develop an [Redacted] (b) (5) However, at the time of OIG's site visit in March 2014, IBWC had not [redacted]

~~(SBU)~~ [Redacted] (b) (5). NIST SP 800-53, Revision 3, states that the organization [Redacted] (b) (5) [Redacted] (b) (5) " IBWC's [Redacted] (b) (5) because of the Information Management Division's [Redacted] (b) (5). Without a [Redacted] (b) (5) unapproved and untested changes to the SCADA systems could occur that would compromise the confidentiality, integrity, and availability of the systems.

~~(SBU)~~ In addition, OIG found that IBWC's [Redacted] (b) (5) NIST SP 800-82[9] states that the [Redacted] (b) (5) Because [Redacted] (b) (5) since our last reporting. Without an [Redacted] (b) (5), IBWC's SCADA systems are more susceptible to security weaknesses and denial of service.

~~(SBU)~~ **Recommendation 2.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5) that includes [Redacted] (b) (5), as

[6] **(U)** IBWC's IT System C&A Inventory Guide, Appendix A, states, "A loss of availability of information could result in severe or catastrophic adverse effect which may cause a severe degradation in or loss of mission capability."
[7] **(U)** Aitheras with subcontractor TruShield.
[8] **(U)** NIST SP 800-53, rev. 3, [Redacted] (b) (5)
[9] **(U)** NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security," June 2011.

required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that it had completed a risk assessment for both SCADA systems, leading to an [Redacted] (b) (5) expected to be completed in FY 2014. IBWC further stated that the [Redacted] (b) (5) would be implemented in 2015.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews and accepts the [redacted]

~~(SBU)~~ **Recommendation 3.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5) as required by National Institute of Standards and Technology Special Publication 800-82.

~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that it had completed a risk assessment for both SCADA systems and that the [Redacted] (b) (5) IBWC further stated that the [Redacted] (b) (5) the end of 2014 and that the [Redacted] (b) (5) will be awarded by the end of FY 2014 and will be implemented in FY 2015.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews the [Redacted] (b) (5)

(U) Finding C. [Redacted] (b) (5) Had Not Been Performed

~~(SBU)~~ In FY 2014, IBWC completed a Business Impact Assessment, an Information System Contingency Plan, and acquired hardware to assist in contingency planning of its GSS. Further, IBWC had established a manual contingency planning process for its SCADA systems. However, IBWC did not [Redacted] (b) (5)

~~(SBU)~~ IBWC had not [redacted]. NIST SP 800-34, Revision 1,[10] states that an organization [Redacted] (b) (5)” IBWC had not performed [Redacted] (b) (5) due to insufficient time between the completion of its [Redacted] (b) (5) and OIG’s site visit. However, by not [redacted]

[10] **(U)** NIST SP 800-34, rev. 1, “Contingency Planning Guide for Federal Information Systems,” Executive Summary, May 2010.

~~(SBU)~~ **Recommendation 4.** OIG recommends that the International Boundary and Water Commission [redacted], as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that it is on target to [redacted] in FY 2014.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives documentation from the [Redacted] (b) (5).

(U) Finding D. [redacted] to Outsider Attacks and Insider Threats

~~(SBU)~~ Although IBWC owns the SBIWTP, the facility is operated by the contractor Veolia.[11] Veolia utilizes a SCADA system to monitor the wastewater treatment process that flows from Tijuana, Mexico. As previously noted, it is the responsibility of IBWC to ensure that the SCADA system used at the [redacted].

~~(SBU)~~ In April 2012, IBWC executed a contract amendment with Veolia that included an additional $100,000 so that Veolia could [Redacted] (b) (5) According to IBWC officials, the $100,000 obligated in FY 2012 remains available until the task is completed. Because Veolia had not performed the required work, IBWC utilized subcontractor TruShield to develop a [redacted] Section 3544(a)(l)(A) of FISMA states:

> The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

~~(SBU)~~ At the time of our fieldwork at SBIWTP in April 2014, no work had been performed by Veolia or TruShield to make the [redacted]. Without IBWC ensuring that the SCADA system at the [Redacted] (b) (5), there is greater risk for outside attacks and insider threats.

~~(SBU)~~ In addition, IBWC included Veolia-owned information technology inventory in the Integrated Logistics Management System, which is strictly for Government-owned assets.

[11] **(U)** Veolia has been under contract with IBWC since October 1, 2010.

[12] **(U)** E-Government Act of 2002, Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (2002).

According to NIST SP 800-53, Revision 3,[13] the organization "develops, documents, and maintains an inventory of information system components that accurately reflects the current information system." This occurred because IBWC tagged all inventory at its facility without first determining ownership. Without determining ownership of the inventory, IBWC is comingling assets that do not belong to the Government resulting in inaccurate inventory which could affect financial reporting.

~~(SBU)~~ **Recommendation 5.** OIG recommends that the International Boundary and Water Commission ensure its [Redacted] (b) (5)

~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that it had excluded the Admin Network from IBWC inventory. In addition, IBWC's Information System Security Manager will review and approve all equipment that supports the SCADA systems [redacted].

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews the contractor-operated system [Redacted] (b) (5)

~~(SBU)~~ **Recommendation 6**. OIG recommends that the International Boundary and Water Commission (IBWC) determine ownership of information technology inventory and update the Integrated Logistics Management System to accurately reflect IBWC's current information system components, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ **Management Response:** IBWC concurred with the recommendation, stating that it had completed a comprehensive inventory validation occurred in FY 2014. IBWC is updating ILMS to ensure that only IBWC inventory is included. IBWC plans on completing this in FY 2014.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG reviews ILMS to determine that only IBWC inventory has been included.

(U) Finding E. IBWC Made Notable Improvements With its Information Security Program

(U) In FY 2014, OIG found that IBWC was in compliance with the FISMA requirements related to risk management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, and security capital planning. In addition, OIG found that IBWC had improved its compliance with FISMA requirements related to contractor oversight and contingency planning. As a result, OIG closed

[13] **(U)** NIST SP 800-53, rev. 3, "CM-8 Information System Component Inventory."

three prior year recommendations related to contractor oversight and one prior year recommendation related to contingency planning. Further, OIG reviewed access controls, personnel security, and physical and environmental protection and found IBWC had implemented sufficient security controls.

(U) OIG would like to call attention to the work and dedication of IBWC officials during the past 6 months to improve IBWC's security program. With top down leadership support, IBWC was able to close 22 of 27 OIG recommendations and IBWC continues to make progress in securing its information systems.

(U) List of Recommendations

~~(SBU)~~ **Recommendation 1.** OIG recommends that the International Boundary and Water Commission (IBWC) [Redacted] (b) (5), as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ **Recommendation 2.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5) that includes [Redacted] (b) (5), as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

~~(SBU)~~ **Recommendation 3.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5) as required by National Institute of Standards and Technology Special Publication 800-82.

~~(SBU)~~ **Recommendation 4.** OIG recommends that the International Boundary and Water Commission [redacted], as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

~~(SBU)~~ **Recommendation 5.** OIG recommends that the International Boundary and Water Commission ensure its [Redacted] (b) (5)

~~(SBU)~~ **Recommendation 6.** OIG recommends that the International Boundary and Water Commission (IBWC) determine ownership of information technology inventory and update the Integrated Logistics Management System to accurately reflect IBWC's current information system components, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Appendix A

(U) Scope and Methodology

(U) The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency's inspector general or an independent external auditor perform annual reviews of the information security program and to report those results to the Office of Management and Budget and the Department of Homeland Security. The Department of Homeland Security uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA. This audit was performed to comply with this requirement.

(U) The Office of Inspector General (OIG), Office of Audits, performed this audit from February 2014 through May 2014. OIG performed site visits to the International Boundary and Water Commission (IBWC) headquarters in El Paso, TX; the South Bay International Wastewater Treatment Plant and field office in San Diego, CA; Nogales International Wastewater Treatment Plant in Nogales, AZ; Amistad Dam and field office in Del Rio, TX; and the General Support System continuity of operations site in Las Cruces, NM.

(U) OIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on its audit objective. OIG believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objective.

(U) To perform this audit, OIG interviewed IBWC senior management, employees, and contractors to evaluate managerial effectiveness and operational controls in accordance with National Institute of Standards and Technology, IBWC, and Office of Management and Budget guidance. OIG observed daily operations, obtained evidence to support OIG conclusions and recommendations, and collected written documents to supplement observations and interviews.

(U) OIG discussed its preliminary findings with IBWC officials on March 27, 2014. OIG provided IBWC with Notice of Findings and Recommendations on May 29, 2014. OIG held an exit conference with IBWC on June 26, 2014.

(U) Work Related to Internal Controls

(U) OIG assessed the adequacy of internal controls by gaining an understanding of the effectiveness of IBWC's information security program as required by FISMA. OIG identified and discussed exceptions with IBWC officials to understand the reasons behind internal control challenges. Through conversations with IBWC officials, OIG gained an understanding of the policies and procedures related to IBWC's information security program. OIG learned how IBWC oversees the development of an information security program to protect information and information systems, to report timely results regarding the security posture of information and information systems, and to implement corrective measures to address previously identified FISMA findings and recommendations. OIG's conclusions on the internal control deficiencies identified during this audit are detailed in the "Audit Results" section of this report.

(U) Use of Computer-Processed Data

(U) The audit team used computer-processed employee background screening data during the audit. To assess the reliability of the data, OIG reviewed documentation related to the background screening. Specifically, OIG traced the background screening documentation to position descriptions to determine which individuals required additional background screening to perform their daily duties. OIG determined that the data were sufficiently reliable to support the conclusions and recommendations presented in this report.

(U) Appendix B

(U) Office of Inspector General FY 2013 Federal Information Security Management Act Report Statuses of Recommendations

~~(SBU)~~ **Recommendation 1.** OIG recommends that the International Boundary and Water Commission update and finalize its risk management framework to include all three tiers of managing risk, as required by National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, Revision 1, and the four risk management steps, as required by NIST SP 800-39.

(U) *Status: Closed March 2014.* The International Boundary and Water Commission (IBWC) provided the Office of Inspector General (OIG) with its risk management framework.

~~(SBU)~~ **Recommendation 2.** OIG recommends that the International Boundary and Water Commission (IBWC) determine the ownership and classification of the South Bay International Wastewater Treatment Plant Admin Network and the Geographic Information System in accordance with Federal Information Processing Standards 199 and update the IBWC Inventory Guide.

(U) *Status: Closed March 2014.* IBWC updated its inventory guide to relinquish the ownership of South Bay International Wastewater Treatment Plant (SBIWTP) Admin Network to a third party and changed the classification of its Geographic Information System, a major application, to be classified as moderate.

~~(SBU)~~ **Recommendation 3.** OIG recommends that the International Boundary and Water Commission (IBWC) develop security authorization packages for all IBWC information systems based on the determination of ownership and classification, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed March 2014.* IBWC developed security authorization packages for its General Support System and its two Supervisory Control and Data Acquisition systems.

~~(SBU)~~ **Recommendation 4.** OIG recommends that the Information Management Division establish a [redacted] for all International Boundary and Water Commission information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and as outlined in NIST SP 800-137.

(U) *Status: This recommendation has been reissued as Recommendation 1 (Finding A) of the FY 2014 report and closed in the FY 2013 FISMA report.*

~~(SBU)~~ **Recommendation 5.** OIG recommends that the International Boundary and Water Commission (IBWC) develop and implement policies and procedures for physical and environmental protection controls for IBWC assets to include information systems at headquarters and at each field office, in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-82.

(U) *Status: Closed March 2014.* IBWC provided OIG with its physical and environmental protection policies and procedures.

~~(SBU)~~ **Recommendation 6.** OIG recommends that the International Boundary and Water Commission develop and implement [redacted], as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed March 2014.* IBWC provided OIG with documentation to support that chain of custody procedures are in place for the access cards and remote gate devices.

~~(SBU)~~ **Recommendation 7.** OIG recommends that the Information Management Division update and implement its Plan of Action and Milestone Directive to include all information systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed March 2014.* IBWC provided its Plan of Action and Milestones for its General Support System and two Supervisory Control and Data Acquisition systems.

~~(SBU)~~ **Recommendation 8.** OIG recommends that the Information Management Division update the Plan of Action and Milestone database [redacted] as stated in the International Boundary and Water Commission Plan of Action and Milestone Directive for all information systems.

(U) *Status: Closed March 2014.* IBWC provided Plan of Action and Milestones which included all elements.

~~(SBU)~~ **Recommendation 9.** OIG recommends that the International Boundary and Water Commission complete a business case/Exhibit 300/Exhibit 53 to obtain the resources required to protect its information systems, as required by National Institute of Standards and Technology Special Publication 800-65.

(U) *Status: Closed March 2014.* IBWC provided documentation showing that the Office of Management and Budget had confirmed that the requirement to complete a business case was not applicable to smaller agencies.

~~(SBU)~~ **Recommendation 10.** OIG recommends that the International Boundary and Water Commission prioritize resources to complete contingency planning documents for all information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-34, Revision 1.

(U) *Status: Closed March 2014.* IBWC provided OIG with a Business Impact Analysis and an Information System Contingency Plan for its General Support System. IBWC's contingency planning for its Supervisory Control and Data Acquisitions are manual controls.

~~(SBU)~~ Recommendation 11. OIG recommends that the International Boundary and Water Commission update, approve, and implement an incident response and reporting policy, to include the correlation of incidents for all information systems, as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, and NIST SP 800-61, Revision 2.

(U) *Status: Closed May 2014.* IBWC provided its incident response and reporting policies for its General Support System and Supervisory Control and Data Acquisition systems.

~~(SBU)~~ Recommendation 12. OIG recommends that the International Boundary and Water Commission (IBWC) implement [redacted], as required by the IBWC Configuration Management Directive and National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: This recommendation has been reissued as Recommendation 2 (Finding B) of the FY 2014 report and closed in the FY 2013 FISMA report.*

~~(SBU)~~ Recommendation 13. OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5) as required by National Institute of Standards and Technology Special Publication 800-82.

(U) *Status: This recommendation has been reissued as Recommendation 3 (Finding B) of the FY 2014 report and closed in the FY 2013 FISMA report.*

~~(SBU)~~ Recommendation 14. OIG recommends that the Information Management Division ensure all new employees receive security awareness training before authorizing access to the network, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed March 2014.* IBWC provided new employee security awareness training completion records.

~~(SBU)~~ Recommendation 15. OIG recommends that the Information Management Division finalize and implement its access control policy, which includes remote access, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed March 2014.* IBWC provided its finalized access control policy which included remote access.

[Redacted] (b) (5)

(U) *Status: Closed March 2014.* IBWC implemented remote access controls to include multifactor authentication, laptop encryption and unique identification of users.

~~**(SBU)**~~ **Recommendation 17.** OIG recommends that the International Boundary and Water Commission (IBWC) ensure all employees that require remote access capabilities for telework complete telework agreements and obtain appropriate approval, as required by IBWC's Telework Directive.

(U) *Status: Closed March 2014.* IBWC provided telework agreements for all telework eligible employees.

~~**(SBU)**~~ **Recommendation 18.** OIG recommends that the International Boundary and Water Commission identify and implement a multifactor authentication solution, to include a process for resetting employee Personal Identification Numbers, for logical access to information systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) *Status: Closed March 2014.* IBWC implemented a multifactor solution, to include a process for resetting employee Personal Identification Numbers, for logical access.

~~**(SBU)**~~ **Recommendation 19.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5), as required by the Federal Information Security Management Act Title III, Section 3544.

(U) *Status: This recommendation has been reissued as Recommendation 5 (Finding D) of the FY 2014 report and closed in the FY 2013 FISMA report.*

~~**(SBU)**~~ **Recommendation 20.** OIG recommends that the International Boundary and Water Commission ensure that its Information Management Division is responsible for the oversight of information technology assets purchased and maintained by the contractor in support of operations at the South Bay International Wastewater Treatment Plant, as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3 and NIST SP 800-82.

(U) *Status: Closed March 2014.* IBWC ensured that its Information Management Division was responsible for oversight of information assets purchased and maintained by the contractor.

~~**(SBU)**~~ **Recommendation 21.** OIG recommends that the International Boundary and Water Commission review and update the appointment letter of the existing contracting officer's representative at South Bay International Wastewater Treatment Plant to include responsibilities for implementing Federal Information Security Management Act (FISMA) compliance for information system assets or appoint another individual the duties for overseeing the FISMA compliance for information system assets.

(U) *Status: Closed March 2014.* IBWC established an additional contracting officer's representative with the responsibility for implementing FISMA.

~~(SBU)~~ **Recommendation 22.** OIG recommends that the International Boundary and Water Commission (IBWC) ensure its Information Management Division reviews and approves software prior to installation on IBWC assets, as required by The Amendment of Solicitation/Modification of Contract M027.

(U) *Status: Closed March 2014.* IBWC relinquished the SBIWTP Admin Network so therefore this recommendation is no longer applicable.

~~(SBU)~~ **Recommendation 23.** OIG recommends that the International Boundary and Water Commission update position descriptions that require background screenings, incorporate appropriate risk designations with the position, and specify the requirement to obtain and maintain the appropriate security clearance.

(U) *Status: Closed March 2014.* IBWC updated position descriptions that required background screenings.

~~(SBU)~~ **Recommendation 24.** OIG recommends that the International Boundary and Water Commission (IBWC) finalize suitability background screenings for both employees and contractors, to include formal adjudication and clearance, as required by IBWC's Personnel Security and Suitability Directive.

(U) *Status: Closed March 2014.* IBWC finalized suitability background screenings for both employees and contractors.

~~(SBU)~~ **Recommendation 25.** OIG recommends that the International Boundary and Water Commission (IBWC), in coordination with the Bureau of Diplomatic Security, Security Infrastructure, Computer Security, and the Bureau of Resource Management, Deputy Chief Financial Officer, Global Financial Management System, suspend IBWC employee access to OpenNet until employee background screenings are completed and adjudicated.

(U) *Status: Closed March 2014.* IBWC suspended employee access to OpenNet for employees who did not have completed and adjudicated background screenings.

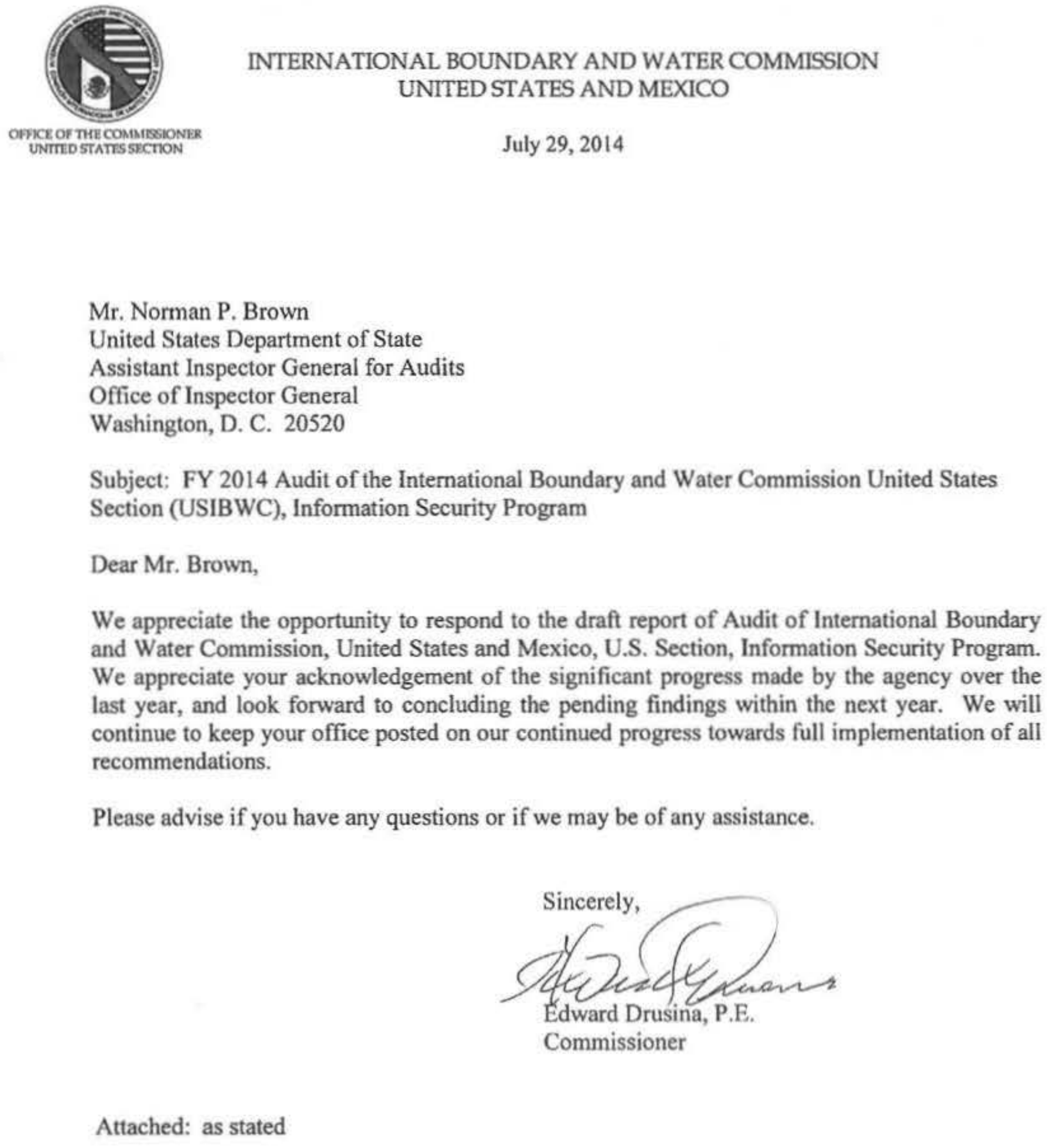
~~(SBU)~~ **Recommendation 26.** OIG recommends that the International Boundary and Water Commission (IBWC), Information Management Division, provide annual certification to the Department of State Bureau of Resource Management indicating that all IBWC OpenNet users fully comply with Department of State requirements concerning OpenNet access.
(U) *Status: Closed March 2014.* IBWC developed a formal certification process with the Department of State Bureau of Resource Management.

~~(SBU)~~ Recommendation 27. OIG recommends that the International Boundary and Water Commission develop and implement a process for conducting and maintaining information system component inventory, to include all information system components concerning the Supervisory Control and Data Acquisition systems, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3, and the Federal Information Security Management Act of 2002.

(U) *Status: This recommendation has been reissued as Recommendation 6 (Finding D) of the FY 2014 report and closed in the FY 2013 FISMA report.*

(U) Appendix C

(U) IBWC Management Responses



INTERNATIONAL BOUNDARY AND WATER COMMISSION
UNITED STATES AND MEXICO

OFFICE OF THE COMMISSIONER
UNITED STATES SECTION

July 29, 2014

Mr. Norman P. Brown
United States Department of State
Assistant Inspector General for Audits
Office of Inspector General
Washington, D. C. 20520

Subject: FY 2014 Audit of the International Boundary and Water Commission United States Section (USIBWC), Information Security Program

Dear Mr. Brown,

We appreciate the opportunity to respond to the draft report of Audit of International Boundary and Water Commission, United States and Mexico, U.S. Section, Information Security Program. We appreciate your acknowledgement of the significant progress made by the agency over the last year, and look forward to concluding the pending findings within the next year. We will continue to keep your office posted on our continued progress towards full implementation of all recommendations.

Please advise if you have any questions or if we may be of any assistance.

Sincerely,

Edward Drusina, P.E.
Commissioner

Attached: as stated

(U) List of Recommendations

~~(SBU)~~ **Recommendation 1.** OIG recommends that the International Boundary and Water Commission [redacted] as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

Response: Concur
The USIBWC is obtaining an [Redacted] (b) (5), which will include IT [Redacted] (b) (5) from a third-party consultant as part of the [Redacted] (b) (5)

~~(SBU)~~ **Recommendation 2.** OIG recommends that the International Boundary and Water Commission [redacted] to include [Redacted] (b) (5) as required by National Institute of Standards and Technology Special Publication 800-53, Revision 3.

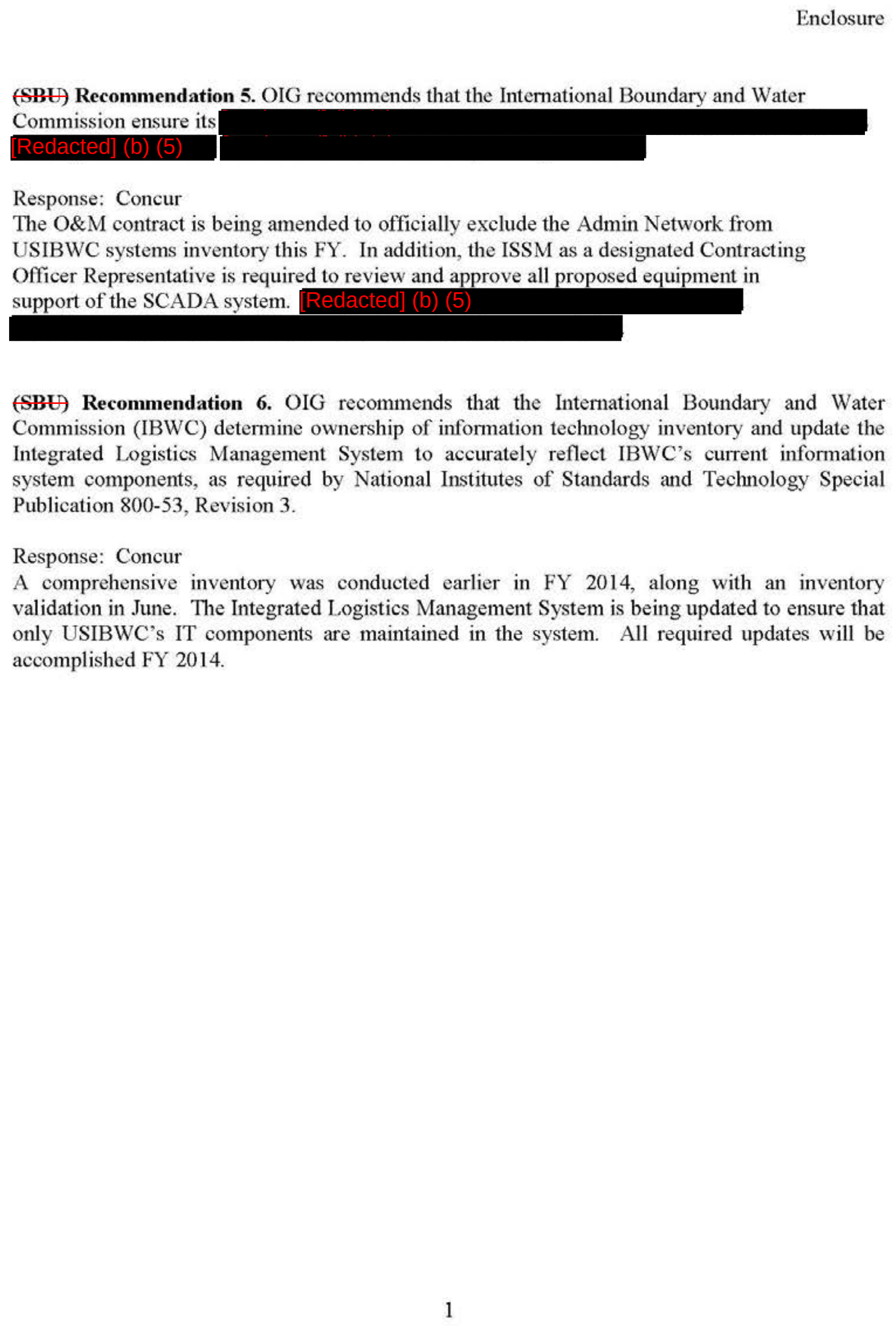
Response: Concur
The USIBWC completed a risk assessment of both SCADA systems, which will lead to the [Redacted] (b) (5) expected to be completed this FY. Implementation is planned for FY 2015, which will include the establishment of a [redacted]

~~(SBU)~~ **Recommendation 3.** OIG recommends that the International Boundary and Water Commission [redacted] as required by National Institute of Standards and Technology Special Publication 800-82.

Response: Concur
The USIBWC completed a risk assessment of both SCADA systems, and the design for the Nogales IWTP is underway. The design for the San Diego IWTP SCADA system will be completed by end of the 2014. The award will be issued by end of FY 2014. The implementation of the [Redacted] (b) (5) will be accomplished in FY 2015.

~~(SBU)~~ **Recommendation 4.** OIG recommends that the International Boundary and Water Commission [Redacted] (b) (5), as required by National Institute of Standards and Technology Special Publication 800-34, Revision 1.

Response: Concur
The USIBWC's plan is still on target to complete a [redacted] in FY 2014.



Enclosure

~~(SBU)~~ **Recommendation 5.** OIG recommends that the International Boundary and Water Commission ensure its [Redacted] (b) (5)

Response: Concur
The O&M contract is being amended to officially exclude the Admin Network from USIBWC systems inventory this FY. In addition, the ISSM as a designated Contracting Officer Representative is required to review and approve all proposed equipment in support of the SCADA system. [Redacted] (b) (5)

~~(SBU)~~ **Recommendation 6.** OIG recommends that the International Boundary and Water Commission (IBWC) determine ownership of information technology inventory and update the Integrated Logistics Management System to accurately reflect IBWC's current information system components, as required by National Institutes of Standards and Technology Special Publication 800-53, Revision 3.

Response: Concur
A comprehensive inventory was conducted earlier in FY 2014, along with an inventory validation in June. The Integrated Logistics Management System is being updated to ensure that only USIBWC's IT components are maintained in the system. All required updates will be accomplished FY 2014.

(U) Major Contributors to This Report

Jerry Rainwaters, Director
Information Technology Division
Office of Audits

Steve Matthews, Information Technology Manager
Information Technology Division
Office of Audits

Kenneth Bensman, Auditor in Charge
Information Technology Division
Office of Audits

FRAUD, WASTE, ABUSE, OR MISMANAGEMENT OF FEDERAL PROGRAMS HURTS EVERYONE.

CONTACT THE
OFFICE OF INSPECTOR GENERAL
HOTLINE
TO REPORT ILLEGAL
OR WASTEFUL ACTIVITIES:

202-647-3320
800-409-9926
oighotline@state.gov
oig.state.gov

Office of Inspector General
U.S. Department of State
P.O. Box 9778
Arlington, VA 22219